Mid-Atlantic Christian University
Office of Information Technology Policy #2

SUBJECT: Information Security

DATE: May 1, 2013

REVISED: 02/11/14; 03/31/2015; April 2020
NEXT SCHEDULED REVIEW: Yearly, February

APPROVED BY BOARD OF TRUSTEES: October 18, 2013

Policy for: All Authorized Users of Mid-Atlantic Christian Information Technology Resources
Procedure for: All Authorized Users of Mid-Atlantic Christian Information Technology Resources
Authorized by: Vice President for Finance
Issued by: Board of Trustees

I. Purpose

Mid-Atlantic Christian University possesses information that is valuable and sensitive and it is important that individuals that handle and interact with this data comply with applicable laws, regulations, University policies, and procedures regarding security and preservation of information. The mishandling of information or exposure of confidential information to unauthorized individuals could cause irreparable harm to the University and could also subject the University to fines or other local, state, and federal sanctions.

II. Policy

Mid-Atlantic Christian University ("University") requires all employees to diligently protect information as required in order to maintain appropriate confidentiality, availability, and integrity. The University maintains baseline information security requirements ("Baselines") that apply to all University-owned or managed information, systems, devices and all devices that access University-owned Resources. More extensive requirements, beyond the baseline requirements, apply to Confidential Information and Mission-Critical Resources.

III. Procedures

INFORMATION SECURITY BASELINES
Baselines are requisite minimum information security standards that must be adhered to and implemented by all University employees and contractors.

1. University employees and contractors may only access information needed to perform your legitimate duties as a University employee and only when authorized by the appropriate Information Custodian.

2. University employees and contractors are expected to ascertain and understand the Sensitivity Level of information to which you have access through training, other resources, or by consultation with your manager or the Information Custodian.
3. All University-owned information, regardless of Sensitivity Level, must be stored on official centralized University file shares.
4. Remote access to University-owned information is only allowed over the official University Virtual Private Network (VPN) service. Third-party VPNs and remote access tools are strictly forbidden.
5. Storing University-owned files on cloud storage providers is forbidden unless the service has been expressly approved by OIT and meets regulatory and compliance standards for information security.
6. University employees and contractors may not in any way divulge, copy, release, sell, loan, alter, or destroy any information except as authorized by the associated Information Custodian within the scope of your professional activities.
7. University employees and contractors must understand and comply with the University's requirements related to personally identifiable information (PII).
8. University employees and contractors must adhere to University's requirements for protecting any computer used to conduct University business or any computers used to transact University business regardless of the Sensitivity Level of the information held on that system.
9. University employees and contractors must protect the confidentiality, integrity, and availability of the University's information as appropriate for the information's Sensitivity Level wherever the information is located or the format of the information (e.g. physical documents, electronic documents, communicated over voice or data networks, exchanged in conversation, etc.)
10. Information deemed Confidential must be handled in accordance with the University's Confidential Information Security Standards.
11. University employees and contractors must safeguard any physical key, ID card or, computer/network account that allows access to University information or resources.
12. University employees and contractors must destroy or render unusable any Confidential Information and/or Resource contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) in accordance with University Data Destruction Procedures.
13. University employees and contractors must report any activities that you suspect may compromise confidential information to your supervisor or to the Office of Information Technology.
14. The obligation to protect confidential information continues after you leave the University.
15. While many federal and state laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact the Office of the President before taking any action.
16. If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this policy annually.

Requirements for any computer used to conduct University business

In order to adequately protect University information systems from compromises, all computers used to conduct University business must be configured using University standards and industry-sanctioned best practices that include but are not limited to the following:

- Configure and use computers in a manner that is compliant with the University's core technology policy, Office of Information Technology F-IT-01 Acceptable Use.
- Require all computer accounts to have strong passwords as defined by the University's Password Standards.
- Define accounts intended for day-to-day computer use as "general user accounts". Accounts that have administrative privileges must only be used for system setup and maintenance.
- If multiple individuals use a system, each should have his or her own login account. Shared accounts are prohibited, except where it is not technically possible to provision individual accounts.
- Computers should be configured to "time out" after no more than 20 minutes of inactivity.
- Users must lock or log off their computers before leaving them unattended.
- Ensure that system and application security updates are applied as soon after being released by the vendor as possible.
- Ensure that anti-virus software is installed and is actively protecting the system.
- Limit the services running on University computers to those needed by the computer user to perform his or her assigned tasks.
- Ensure that any system is configured to keep a record of:
    - Who attempted to log into the system (successfully and unsuccessfully) and when,
    - When they logged out,
    - Administrative activity performed.

Requirements for Personally Owned Computing Devices

Risks, Liabilities, Disclaimers for Requirements for Personally Owned Computing Devices and Bring your Own Device Posture.

1. The University does not condone the use of personally owned computing devices (“POCD”) for University-related business unless no other reasonable alternative exists.
2. At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device.
3. The University does not provide support for POCD including, but not limited to:
    a. Troubleshooting device performance or hardware problems
    b. Troubleshooting software applications or cloud services
    c. Installing OS upgrades, OS patches, or University-owned software on POCD
    d. Backing up device data or migrating data to a new device
    e. Removing malware or spyware
4. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems.
5. The University shall NOT be liable for the loss, theft, or damage of POCD. This includes, but is not limited to, when the device is being used for University business, on University time, or during University-related business travel.

6. The University reserves the right to implement technology such as Mobile Device Management to enable the removal of University-owned data.
7. Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. The University will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.
8. The University reserves the right to perform security scans against any POCD that accesses University networks in accordance to with Office of Information Technology Policy F-IT 01 Acceptable Usage of Information Technology Resources. OIT may, without notification, prevent or ban POCD that disrupt any Resources or are used in a manner that violates any University policies.

Responsibilities related to and the use of Personally Owned Computing Devices

1. The use of PCODs must not disrupt the use of Resources.
2. Employees must not install software that is licensed to the University on PCOD.
3. Employees must not store University-owned Confidential Information on POCD.
4. Employees must destroy, remove or return all data, electronic or otherwise belonging to the University, once their relationship with the University ends or once they are no longer the owner or primary user of the POCD. (E.g. the sale or transfer of a POCD to another person)
5. Employees must notify OIT of any theft or loss of a POCD containing University-owned data.
6. At no time may a POCD be connected to the secure University networks (E.g. MACU) without prior approval.

ROLES AND RESPONSIBILITIES

Departmental Managers

In addition to complying with the Baselines, departmental managers and supervisors must:

- Ensure that departmental procedures support the objectives of confidentiality, integrity, and availability defined by the Information Custodian and designees, and that those procedures are followed.
- Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands his or her information security-related responsibilities.

Technology managers

In addition to complying with the policy requirements defined for all employees and contractors, and managers, those who manage computing and network environments that capture, store, process and/or transmit University information, are responsible for ensuring that the requirements for confidentiality, integrity, and availability as defined by the appropriate Information Custodian are being satisfied within their environments. This includes:

- Understanding the Sensitivity Level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.

- Developing, implementing, operating and maintaining a secure technology environment and Information Security Program that includes:
    - A cohesive architectural policy,
    - Product implementation and configuration standards,
    - Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Custodians, and
    - An effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.
    - Ensuring that staff members understand the Sensitivity Levels of the data being handled and the measures used to secure it.
    - Evaluating and assessing risks related to information security

Information custodians
University-owned information must be protected against unauthorized exposure, modification, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws, the University's contractual obligations, University policies and procedures, and with the information’s significance to the University. Achieving this objective requires that:

- The information's Sensitivity Level must be defined to convey what level of protection is expected to all employees/agents who are authorized to access the information.
- The individuals who should have access to confidential information must be identified, either by role or by name.
- For purposes of managing information, the University's various types of information must be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, undergraduate student records, graduate student records, personal data regarding alumni, financial records). Each collection must be "managed" by an individual known as an “Information Custodian,” who must:

    - Define the collection’s Sensitivity Level consistent with this policy,
    - Convey the collection’s requirements to the managers of departments that will have access to the collection,
    - Work with department heads to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).
    - The custodian of an information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. Each Information Custodian may designate one or more individuals on his or her staff to perform the above duties. However, the Information Custodian retains ultimate responsibility for their actions.

- In addition to complying with the requirements listed above, Information Custodians are responsible for:

- Working with the Office of Information Technology to understand the restrictions on the access and use of information as defined by federal and state laws and contractual obligations.
- Segregating the information for which he or she is responsible into logical groupings, called information collections,
- Defining the confidentiality, integrity, and availability requirements (Sensitivity Level) for each of his or her Information Collections.
- Conveying in writing the Sensitivity Level of each Information Collection for which he or she is responsible to the managers of departments that will have access to the collection,
- Working with department managers to determine what users, groups, roles or job functions will be authorized to access the Information Collection and in what manner (e.g., who can view the information, who can update the information).

INFORMATION/RESOURCE SENSITIVITY LEVELS AND CLASSIFCATION

All Users must be aware of the classification of the various types of University information to which they have access in order to determine the proper controls for safeguarding the information. Regardless of classification, the integrity and accuracy of all information must be protected. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, printed report) must have the same classification regardless of format. Only two (2) Sensitivity Levels are to be used when classifying information:

1. Confidential (Level 1)
2. Public (Level 2)

Confidential (Level 1)

Information that has been determined by institutional information stewards to require the highest level of privacy and security controls. Currently, any information that contains any of the following data elements, when appearing in conjunction with an individual’s name or other identifier, is considered confidential (level 1) information:

- Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)
- Student “education records,” as defined by the Family Educational Rights and Privacy Act (FERPA).
- “Customer record information,” as defined by the Gramm Leach Bliley Act (GLBA).
- “Card holder data,” as defined by the Payment Card Industry Data Security Standard (PCI DSS).
- Information designated by any University policy, Federal or state law, or any other compliance obligation as Personally Identifiable Information (PII)

    - All Personally Identifiable Information in the possession of the University is considered Confidential unless:

    - The information is designated as “Directory Information” by the appropriate Information Custodian; or
    - The Information Custodian has otherwise authorized its disclosure.

  - The University requires that the following pieces of PII may not be collected, stored or used except in situations where there is legitimate business need and **no reasonable alternative**:

    - Social Security Number,
    - Date of birth,
    - Place of birth,
    - Mother’s maiden name,
    - Credit card numbers,
    - Bank account numbers,
    - Income tax records, and
    - Driver’s license numbers.

Confidential Information also includes any other information that is protected by University policy or federal or state law from unauthorized access. Confidential Information must be restricted to those with a legitimate business need for access. Examples of Confidential Information may include, but are not limited to, Social Security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, student disciplinary records, information security records, and information file encryption keys.

Please note that some data elements classified as confidential (level 1) institutional information are subject to legal or regulatory requirements that go beyond those given here. Such requirements for regulated information are expected to be fulfilled, along with these University requirements.

For example, credit card numbers and how the University handles credit card transactions are subject to the Payment Card Industry Data Security Standard (PCI DSS).

Public (Level 2) Information

Public Information includes all information made or received by the University that does not constitute Confidential Information. Confidential Information that is disclosed without proper authorization does not, by virtue of its disclosure, become Public Information.

This policy does not limit these safeguard provisions to only these data elements and types, but establishes the foundational rules beneath which no steward or custodian may allow.

Mission-Critical Resources

In addition to Sensitivity levels for information, the University designates some Resources as Mission-Critical.

Mission-Critical Resources must be protected from accidental or intentional unauthorized modification, destruction, or disclosure. The University also requires members of its faculty, staff, and student body to protect the University’s Mission-Critical Resources by adhering to the this policy and its accompanying standards and procedures. Users who are third-party contractors and vendors must also be made aware of this policy and their responsibilities for safeguarding the University's Mission-Critical Resources.

A Mission-Critical Resource includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Mission-Critical resources for Information Security purposes include information assets, software, hardware, and facilities that are vital for University business. For example, the University's financial software and student information system are Mission-Critical Resources.

Mission-critical computer systems and the infrastructure required to support them must be installed in access-controlled areas. In addition, the area in and around a computer facility housing Mission-Critical Resources must afford protection against fire, water damage, and other environmental hazards, such as power outages and extreme temperature situations. Each University business unit housing Mission Critical Resources is required to establish procedures to provide emergency access to those Resources in the event that the assigned Custodians are unavailable, or when operating in an emergency.

MANAGING INFORMATION

Managing and Processing Confidential Information

No one may access information or resources that has been classified as Confidential or Mission-Critical without authorization by the appropriate Information Custodian. Any system storing or processing Confidential Information must be documented and tracked by the Office of Information Technology and assigned to an Information Custodian. Confidential Information must be protected at all times against possible unauthorized disclosure, access, or alteration.

For information and resources classified as Confidential or Mission-Critical, the following procedural and system-level controls must be in place:

Confidential Information at Rest

Confidential Information at Rest must be encrypted whenever possible. Where feasible, use full-disk encryption.

Confidential Information must be stored on University-managed file shares. Permissions to network drives are managed by the Office of Information in coordination with Information Custodians.

The storage of University-owned Confidential Information on non-University owned Resources is forbidden.

Confidential Information must not be stored on Portable Media. However, if legitimate and unavoidable business needs require Confidential Information to be stored on Portable Media the information must be encrypted.

Confidential Information stored on University-owned fixed computing devices (e.g. workstations and servers) should be encrypted whenever possible.

External media and mobile computing devices containing Confidential Information must never be left unattended in unsecured areas.

Confidential information must never be available from publically accessible computers or kiosk.

Confidential Information in Transit

Technical security mechanisms must be employed to guard against unauthorized access to Confidential Information that is transmitted over a communications network. When transmitting Confidential Information to third parties, such as outside vendors, a signed contractual or formal business agreement with the third party, approved by the University counsel, must be in place that ensures the protection of Confidential Information and clarifies the liability for any data compromise or security breach. Downloading and uploading Confidential Information between systems must be strictly controlled.

Encryption is not required for a University employee who uses an on-campus workstation, with a wired connection to the University network, to transmit a document to another University User or to save a document containing PHI or PII to his/her University-managed network folder.

The transmission of Confidential Information over public Wi-Fi (e.g. hotel wireless, restaurant wireless University guest wireless network), using a home internet connection, or any other connection not directly managed by the University must be conducted via while using the University's VPN service.

Using the University's secure wireless network (MACU) or wired network does not require the use of a VPN connection to transmit Confidential or Mission-Critical Information or Resources.

Confidential Information must never be handled through Instant Messaging (IM) or Peer-to-Peer (P2P) file sharing software or devices. In addition, P2P software is expressly prohibited on all University-owned resources.

Confidential Information must not be copied, printed, or stored in a manner that would leave it vulnerable to unauthorized access.

Using, Maintaining, and Managing Confidential Information

Any publication of Confidential Information must be in accordance with University Policies and any applicable federal and state law. In addition, any such publication must have the advance written approval of the respective Information Custodian with consultation, as necessary, with the University Counsel.

Confidential Information must not be uploaded to or posted on any web site, blog or social media site, including web sites officially maintained by the University, unless it is protected in a way that permits the Confidential Information to be accessed and seen only by those individuals authorized to access and see it.

When verbally communicating Confidential Information to other authorized personnel, individuals must be aware of their surroundings to prevent unauthorized disclosure of Confidential Information.

Any other use of Confidential Information, whether in duplicate or original form, must be in accordance with University Policy

Disposal and Destruction of Confidential Information

The destruction of Confidential Information must be in accordance with departmental record retention schedules and consistent with the standards defined by the Office of Information Technology for Media Destruction.

Subpoenas and Other Compulsory Requests (Disclosure)

Many of the federal and state laws described in this policy create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders, and other compulsory requests from law enforcement agencies. Employees who receive such compulsory requests should contact the Office of the President before taking any action.

Access Controls for Confidential Information and Mission-Critical Resources

Physical and electronic access to Confidential Information and Mission-Critical Resources must be controlled. Mechanisms to control access to Confidential Information and Mission-Critical Resources include (but are not limited to) the following methods:

- Authorization Access controls should be appropriate to the Sensitivity Level of the data as outlined in this policy.
- Unique user identification (MACUID) and authentication is required for all systems that store, process, or access Confidential Information. Users will be held accountable for all actions performed on the system with their user identification.

A Custodian of that Confidential Information must control access to areas in which Confidential Information is stored. Only authorized personnel may access secure areas and only when there is a legitimate business need. The following physical controls must be in place:

- Mission-Critical computer systems and the infrastructure required to support them must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards, such as power outages and extreme temperature situations.
- Servers on which Confidential Information is stored must be kept in a secure area to protect against unauthorized access.
- Computing Devices that contain or have access to Confidential Information, including any Portable Devices, must be secured against use, including viewing, by unauthorized individuals. In particular, workstations and mobile devices must be positioned to minimize unauthorized viewing of Confidential Information.

- Physical safeguards, such as locating workstations in controlled-access areas or installing covers or enclosures, should be employed to preclude passerby access to Confidential Information.

Remote Access
Confidential Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the University network.

Emergency Access to Mission-Critical Devices and Data
Each University business unit is required, in cooperation with the Office of Information Technology, to establish procedures to provide emergency access to Mission-Critical Devices and applications in the event that the assigned Custodians or are unavailable, or when operating in an emergency.

INCIDENT MANAGEMENT AND REPORTING

University employees and students must immediately report all known or suspected security breaches to the Office of Information Technology and to the individual's manager or other appropriate university official. In accordance with the University whistleblower policy (F-11 Whistleblower), the University prohibits retaliation against a member of the University community for making a good faith report of a potential University-related legal or policy violation.

The Office of Information Technology, in consultation with the Office of the President and University counsel, will notify affected all parties affected by a security breach in accordance with the North Carolina Identity Theft Protection Act of 2005

The Office of Information Technology reserves the right to remove a user's network access in order to mitigate the risk to the University network during an Information Security Incident. Network access will be removed for users if their continued access of University network resources has the potential to impact the security and availability of the University network and information technology resources.

BACKUP AND RECOVERY

Information Custodians must ensure that the systems and information for which they are responsible are recoverable within a reasonable time period. Each University business unit operating Mission-Critical Resources is required to develop and maintain a plan for responding to a system emergency and to Information Security Incidents.

- Backup media must be encrypted. A disaster recovery plan must be developed and documented in coordination with the Office of Information Technology
- Backup data/media must be periodically stored in a secure off-site location Off-site storage locations should be compliant with the commercial standards for environmental controls.

TRAINING AND AWARENESS

Each new University employee will be trained on the Acceptable Use Policy and University Information Security Policy as they relate to individual job responsibilities. Such training will include information regarding controls and procedures to prevent employees from providing data to an unauthorized individual.

The Office Information Technology must make annual security awareness disclosures to all employees to ensure that all employees are aware of the University's policies and procedures for Information Security.

CONTRACTUAL OBLIGATIONS

Agreements protecting another entity's information

University employees are responsible for complying with the terms of contracts or agreements that may limit the ability to disclose confidential information belonging to (or collected on behalf of) another organization. Employees are expected to educate themselves about the limitations imposed on the information to which they have access, including contractual obligations. Some examples of these arrangements are:

- Non-disclosure agreements
- Non-disclosure agreements where the external entity shares pre-release product information,
- End user licensing agreements associated with commercial software, shareware, freeware and other software,
- Contractual obligations with external entities requiring compliance with security standards for an industry or association. The credit and debit card industry requires that we comply with data security standards known as PCI-DSS.

Access to Information under Vendor Agreements/Protecting University Data

When negotiating contracts with external entities, University employees should consider whether there are any alternatives to giving members of the other organization access to University databases or to other filing systems containing confidential information.

If such access is necessary, agreements that provide the outside entity with access must ensure that the employees/agents of the entity are required to maintain confidentiality consistent with the University's obligations and interests. In addition, outside employees/agents should be contractually obligated to implement data protection and security measures that are commensurate with the University's practices.

COMPLIANCE AND SANCTIONS

Failure to adhere to this Policy and its Procedures and Standards may put University information assets at risk and may have disciplinary consequences for employees up to and including termination of employment.

Students who fail to adhere to this Policy and the Procedures and Standards will be referred to the disciplinary committee.

Contractors and vendors who fail to adhere to this Policy and its Procedures and Standards may face termination of their business relationships with the University.

IV. Published: Policy Manual

V. Reasons for Revisions

VI. Appendices

Relevant University Policies, Standards, and Procedures	
F-IT 01 Acceptable Use	
F 10 Document Retention and Destruction	
F 11 Whistleblower	
University Backup and Recovery Procedures	On file in the Office of Information Technology
University Data Destruction Procedures	On file in the Office of Information Technology
University Password Standard	On file in the Office of Information Technology

Definitions	
Authorized Use	Authorized Use of Resources is use that the University determines, in its sole and exclusive discretion, is consistent with the education, research, and mission of the University, consistent with effective departmental or divisional operations, and consistent with this policy.
Authorized Users	Authorized Users may include: • Current faculty, staff, and students of the University • Anyone connecting to a public information service through the use of University Resources • Others whose access furthers the mission of the University, and whose usage does not interfere with general access to Resources, as determined by the University in its sole and exclusive discretion
Data at Rest	Data that is commonly located on desktops and laptops, in databases and on file servers. In addition, subsets of data can often be found in log files, application files, configuration files, and many other places.
Data in Transit	Data in transit is data that is moving across public or “untrusted” networks such as the Internet and/or data that is moving within the confines of private networks such as the local University network.
Directory Information, Current and past students	The University defines the following to be “Directory Information” that may be shared: • Name • Address (While FERPA permits sharing address information, the Custodians require that it be treated as “Internal” and not disclosed absent compelling reason) • Telephone number • E-mail address • Photo

	• Dates of attendance • Major field of study • Participation in officially recognized activities, organizations and athletic teams • Weight and height of members of athletic teams • Degrees and awards • Academic institution attended immediately prior to Princeton University.
Directory Information, Faculty and Staff	The following information about current and former staff and faculty is considered to be “Directory Information”: • Name • Dates of his or her affiliation with the University • Office address and phone number • E-mail address • Title and/or job function For information about providing references for former employees or faculty, please contact Human Resources or the Dean of the Faculty office.
Mission-Critical Resource	Any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes.
Personally Identifiable Information (“PII”)	Information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc.
Personally Owned Computing Device	Devices used by Authorized Users that are not owned by the University.
Portable Media	Portable media includes any portable device that is capable of storing data (e.g. flash drives, portable hard drives, CDs, DVDs, tape storage, smartphones, tablets, laptop computers, etc.)
Resources	Resources - Resources means the University's computing, network and, information technology Resources, including without limitation all data and information in electronic format or any hardware or software that makes possible, in the broadest possible sense, the processing, transmission, storage or use of such information.
Sensitivity Levels	The University classifies information and resources into two sensitivity levels: 1. Confidential 2. Public
Virtual Private Network (“VPN”)	VPN is a service that allows for secure, remote connection to University resources.

Relevant Legislation and Statutes

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)	This law impacts every office and employee of the University who comes in contact with student records. All University employees are expected to be familiar with the requirements of FERPA and its application to their work. Enacted in 1974, FERPA (also known as the Buckley Amendment) affords students certain rights with respect to the student’s “education records.” As defined by FERPA, the term “education records” encompasses a broad range of materials and information such as disciplinary, financial and academic records created during a given student’s enrollment and maintained by the University, whether in paper form, in databases or other means of storage. In particular, FERPA provides that “education records” and personally identifiable information contained therein may not be disclosed without the written consent of the student. Violations of FERPA may result not only from the unauthorized disclosure of education records but also from the failure to exercise due care in protecting such records against unauthorized access from outsiders. However, even in the absence of express student consent, FERPA permits disclosure of education records to University employees who have a legitimate interest in the student and to outside parties in a variety of circumstances, such as those where public health or safety are at issue.
The “Red Flags Rule”	The University’s loan programs are subject to the Federal Trade Commission’s (FTC) Red Flag Rule, which implements sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACT) of 2003. Compliance requires that the University take steps to protect the identity of those to whom it extends credit and that it develop and implement an identity theft program for new and existing accounts. Adherence is mandatory for “creditors or financial institutions that provide covered accounts”. In addition, the regulation requires users of consumer reports to develop reasonable policies and procedures to react to a notice of an address discrepancy or a fraud alert. This provision applies when credit or background checks are done on prospective employees or when credit checks are requested for new loan applicants or assessment of delinquent account holders. Further information is available from the University’s Identity Theft Prevention Coordinator.
Payment Card Industry Data Security Standards (PCI-DSS)	To reduce their losses due to credit card fraud, five members of the payment card industry, Visa, Master Card, American Express, Discover and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry’s Data Security Standard, or "PCI-DSS." PCI-DSS is enforced through the contracts that Princeton University, as a merchant account holder, has with our merchant bank, i.e., the financial institution that serves as a liaison between Princeton University merchants and the payment card companies. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card

	privileges, and fines in cases where a credit or debit card account is compromised.
Computer Fraud and Abuse Act (CFAA)	Enacted in 1984 (and revised in 1994), the CFAA criminalizes unauthorized access to a “protected computer” with the intent to defraud, obtain any information of value or cause damage to the computer. Under the CFAA, a “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or that is used by or for a financial institution or the government of the United States. For example, the act of “hacking” into a secure web site from an out-of-state computer may violate the CFAA.
The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA))	Enacted in 1999, the GLBA requires financial institutions to carefully protect customers’ financial information. Universities are “financial institutions” by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) “safeguarding” rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure. The University has designated information security program managers in the business units that handle financial information, identified risks to the security of financial information, and is developing security programs to protect against risks. As the privacy standards of GLBA must be followed for all non-student financial information, the University is developing a privacy policy to comply with GLBA and will make required privacy notifications to non-student customers whose financial information is obtained. More information is available on the Federal Trade Commission website.
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009	In February 2009, the American Recovery and Reinvestment Act of 2009 (“ARRA”) was enacted. Title XIII of the ARRA, The Health Information Technology for Economic and Clinical Health Act (“HITECH Act” or the “Act”), imposed new federal security breach notice requirements and added numerous new privacy and data security restrictions for covered entities and their business associates under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Princeton, as a sponsor of self-insured group health plans, has certain offices that are required to comply with HIPAA and therefore must comply with the HITECH Act. The HITECH Act created numerous modifications to the HIPAA Privacy and Security Regulations, such as further restricting permitted disclosures and requiring additional record keeping for disclosures, as well as requiring changes to agreements with business associates. The Act also creates new federal security breach notice laws that apply to all personal information held by a health plan sponsor such as Princeton. These laws require notice to individuals, government agencies, and, in some cases, the media.
The Technology, Education, and Copyright Harmonization Act (TEACH	Enacted in 2002, the TEACH Act relaxes certain copyright restrictions so that accredited, non-profit colleges and universities may use multimedia content for instructional purposes in technology-mediated settings. However, the TEACH Act carries a number of security requirements

Act)	designed to ensure that digitally transmitted content will be accessible only to students who are properly enrolled in a given course.
North Carolina Identity Theft Protection Act of 2005	Enacted in 2005, the North Carolina Identity Theft Protection Act of 2005 affords certain protections to individuals and requires that businesses within North Carolina take reasonable steps to protect the information of its information. Additionally, this act requires that the University notify affected users of security breaches.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Enacted in 1996, HIPAA imposes obligations on health plans, health care clearinghouses, and health care providers to protect health information when electronically transmitted. As a provider of self-insured group health plans, the University is subject to certain HIPAA requirements. Therefore, certain offices must take steps to appropriately manage contracts with business associates, complete training on applicable privacy policies and procedures and/or complete a confidentiality acknowledgement. HIPAA may also apply to certain research activities such as the collection and use of personally identifying health information from patient populations in clinical settings. Further information regarding compliance with HIPAA is available through the University's Privacy Officer, Director of Risk Management, or from the Office of the General Counsel.
Electronic Communications Privacy Act (ECPA)	Enacted in 1986, the ECPA broadly prohibits (and makes criminal) the unauthorized use or interception of the contents or substance of wire, oral or electronic communications. In addition, the ECPA prohibits unauthorized access to or disclosure of electronically stored communications or information. Such prohibitions may apply to University employees who willfully exceed the scope of their duties or authorizations by accessing certain databases housed within the University system. The ECPA does not, however, prohibit the University from monitoring network usage levels and patterns in order to ensure the proper functioning of its information systems.